

PATENT

Atty. Dkt. No. ATT/2000-0008

REMARKS

In view of the above amendment and the following discussion, the Applicant submits that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102. Thus, the Applicant believes that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-18 UNDER 35 U.S.C. § 102

The Examiner has rejected claims 1-18 in the Office Action under 35 U.S.C. § 102 as being anticipated by Coss (US Patent 6,098,172, issued August 1, 2000, herein referred to as "Coss"). In response the Applicant has amended independent claims 1, 6, 10 and 15. As such, Applicant respectfully traverses the rejection.

Coss teaches a method and apparatus for a computer network firewall that can be configured to utilize "stateful" packet filtering. The firewall functions by applying any one of several distinct sets of access rules for a given packet. However, stateful packet filtering may be implemented by caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. (See Coss, Abstract; Column 2, lines 5-18; Col. 5, Lines 46-49)

The Examiner's attention is directed to the fact that Coss fails to teach or to suggest the novel concept of authorizing subsequent inbound packet traffic destined for the process group network address, wherein said process group network address is assigned to a transient host process group, as positively claimed by the Applicant. Specifically, Applicant's amended independent claims 1, 6, 10 and 15 positively recite:

1 A method of processing packets at a firewall in a packet-switched network comprising:
receiving an outbound packet from a process group network address; and
authorizing subsequent inbound packet traffic destined for the process group network address, wherein said process group network address is assigned to a transient host process group. (Emphasis Added.)

6. A method of processing packets at a host which are destined for a firewall in a packet-switched network comprising the steps of:

PATENT

Atty. Dkt. No. ATT/2000-0008

assigning a process group network address to a first outbound packet commencing a transient process;
transmitting the outbound packet to a firewall on its path to its destination in a packet-switched network;
receiving inbound packets addressed to the process group network address; and
authorizing, based on the process group network address and associating inbound packets addressed to the process group network address with the transient process. (Emphasis Added.)

10. A computer readable medium containing executable program instructions for performing a method on a firewall connected to a packet-switched network comprising the steps of:

receiving an outbound packet from a process group network address; and
authorizing subsequent inbound packet traffic destined for the process group network address, wherein said process group network address is assigned to a transient host process group. (Emphasis Added.)

15. A computer readable medium containing executable program instructions for performing a method on a host connected to a packet-switched network comprising the steps of:

assigning a process group network address to a first outbound packet commencing a transient process;

transmitting the outbound packet to a firewall on its path to its destination in a packet-switched network;

receiving inbound packets addressed to the process group network address; and

authorizing, based on the process group network address and associating inbound packets addressed to the process group network address with the transient process (Emphasis Added.)

Applicant's invention teaches the novel concept where a plurality of transient processes or host process groups are assigned unique temporary process group network addresses. When the firewall receives an "outbound" packet having one of these process group network addresses, the firewall will then authorize further "inbound" packets addressed to the particular process group network address. Thus, the firewall advantageously need not know the details of the particular protocol in deciding whether to permit the inbound traffic, e.g., the firewall does not need to look at the port number or the content of the inbound packet. This novel approach greatly

PATENT

Atty. Dkt. No. ATT/2000-0008

accelerates the passage of inbound packets by the firewall. Thus, Applicant's invention discloses and claims a firewall this is capable of authorizing subsequent inbound packet traffic destined for the process group network address, wherein said process group network address is assigned to a transient host process group or a transient process.

In contrast, this novel concept is completely absent in Coss. Coss only teaches a method and apparatus for a computer network firewall that can be configured to utilize "stateful" packet filtering. The firewall functions by applying any one of several distinct sets of access rules for a given packet. However, stateful packet filtering may be implemented by caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. Namely, Coss' invention derives computational efficiency by caching some of rule processing results to avoid having to apply the set of rules repeatedly. However, Coss teaches that the firewall must extract the session key from the IP header and then if there is a match, it will then determine a destination interface and a destination address of the packet to determine the destination domain. As such, Coss must determine, at minimum, three separate items of information: a session key, a destination interface and a destination address, before the packet can be forwarded. (See Coss, Column 7, lines 4-52). Thus, Coss' approach is to use a session key for authorizing the passage of packets by the firewall, whereas Applicant's invention uses process group network address for authorizing the passage of packets by the firewall.

Second, Coss describes that the destination address is a local area network address. Coss then cites Figure 4 to show the relationship between the session key and the "hardware address". Thus, the destination address of Coss is the hardware address of the host.

In contrast, Applicant's invention assigns a unique process group network address to each transient process or process group. Thus, clearly Applicant's process group network address is not the hardware address of the host as disclosed by Coss.

Therefore, Applicant respectfully submits that amended independent claims 1, 6, 10 and 15 are clearly patentable and not anticipated by Coss. Furthermore, dependent claims 2-5, 7-9, 11-14 and 16-18 depend, directly or indirectly, from claims 1, 6, 10 and 15 and recite additional limitations. As such, and for the exact same reason set forth

PATENT

Atty. Dkt. No. ATT/2000-0008

above, the Applicant submits that claims 2-5, 7-9, 11-14 and 16-18 are also patentable and not anticipated by Coss.

Conclusion

Thus, the Applicant submits that all of these claims now fully satisfy the requirements of 35 U.S.C. §102. Consequently, the Applicant believes that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

11/4/04



Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Moser, Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702